

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-087078

(43)Date of publication of application : 31.03.1995

(51)Int.Cl.

H04L 9/00
G06F 13/00
G09C 1/00
H04L 9/06
H04L 9/10
H04L 9/12
H04L 9/14

(21)Application number : 05-180917

(71)Applicant : ROORERU INTELLIGENT SYST:KK

(22)Date of filing : 25.06.1993

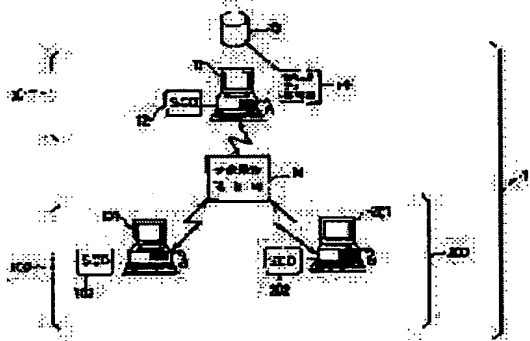
(72)Inventor : TORIKAI MASAMICHI
FUJII MIKIO

(54) INFORMATION TRANSMISSION SYSTEM

(57)Abstract:

PURPOSE: To attain the transmission reception of information in a complete security state by connecting a ciphering device to a terminal device, applying ciphering processing to a specific user password with a ciphering algorithm, creating a terminal identification key able to specify the terminal device, confirming the validity of the terminal device based on the terminal identification key and sending the information.

CONSTITUTION: A security server means 10 is connected to lots of file server means 100 and file receiver means 200 by utilizing a public communication network N. The security server means 10 uses a central device 11 and a ciphering device 12 connecting to the central device 11 to attain transmission reception of ciphered information between terminal devices 101, 201 of each file server means 100 and each file receiver means 200. Furthermore, the file server means 100 includes terminals devices 101... and each ciphered device 102 connecting to each terminal device 101 and registers each terminals device 101 and attains transmission/reception if ciphered information.



LEGAL STATUS

[Date of request for examination] 17.04.2000

[Date of sending the examiner's decision of rejection] 19.08.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

BEST AVAILABLE COPY

(11)特許出願公開番号

(43)公開日 平成7年(1995)3月31日

H04L 9/00

【特許請求の範囲】

【請求項 1】 予め登録された正当な端末デバイス間で情報を伝送する情報伝送システムであって、前記の端末デバイスには、暗号デバイスを接続しており、個々のユーザ暗証を暗号アルゴリズムにより暗号化処理して前記の端末デバイスを特定する端末識別キーを創成し、当該端末識別キーにより端末デバイスの正当性を確認した後、情報を伝送するように構成した情報伝送システム。

【請求項 2】 端末デバイスを備えたファイルサーバ手段と、ファイルレシーバ手段との間に同様の端末デバイスを備えたセキュリティサーバ手段を介在させて、情報を授受するようにした請求項 1 記載の情報伝送システム。

【請求項 3】 前記セキュリティサーバ手段においては、前記ファイルサーバ手段と、ファイルレシーバ手段とに乱数キーを送信する手段と、前記ファイルサーバ手段とファイルレシーバ手段とから返信された端末識別暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより前記ファイルサーバ手段と、ファイルレシーバ手段の暗号化端末識別キーを登録する手段を備えており、前記ファイルサーバ手段と、ファイルレシーバ手段においては、各端末識別キーの創成と、各端末識別キーを前記乱数キーによって暗号化して端末識別暗号キーを創成して、これを前記セキュリティサーバ手段に返信する手段とを備えた請求項 1 又は 2 記載の情報伝送システム。

【請求項 4】 前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して照合キーを生成すると共に、前記ファイルサーバ手段から返信された端末識別キーによって乱数キーを暗号化した確認キーと、当該照合キーとを照合させて、前記ファイルサーバ手段の端末デバイスの正当性を認証する手段を具備してなる請求項 1 乃至 3 記載の情報伝送システム。

【請求項 5】 前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して暗号化処理キーを求めると共に、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して復号化処理キーを生成する手段を備えており、当該暗号化処理キーをファイルサーバ手段に送信し、ファイルサーバ手段においては、その端末識別キーにより前記暗号化処理キーを復号化して暗号化実行キーを生成し、当該暗号化実行キーにより機密ファイルを暗号化して、前記セキュリティサーバ手段に返信する手段を含んでいる請求項 1 乃至 4 記載の情報伝送システム。

【請求項 6】 前記セキュリティサーバ手段にあって

は、前記暗号化ファイルと共に、前記復号化処理キーをファイルレシーバ手段に送信する手段を含んでおり、ファイルレシーバ手段にあっては、その端末識別キーにより復号化処理キーを復号化して復号化実行キーを求め、当該復号化実行キーにより、暗号化ファイルを復号化処理して平文情報を受領する手段を備えている請求項 1 乃至 5 記載の情報伝送システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、公衆電話回線などの通信網を利用した情報伝送技術において、登録された特定の端末デバイス間においてのみ情報の伝送を保障する情報伝送システムに関するものである。

【0002】

【従来の技術】 従来、トレードシークレットなどの貴重な機密情報を安全に保管し、又は、伝送するために平文情報を暗号化処理し、パソコンなどの端末デバイスを公衆電話回線によって接続して授受する技術は広く活用されており、この際、情報伝送の当事者の確認は、通常例えば、IDコードやパスワードなどによっているところである。

【0003】 しかしながら、悪意の第三者が、不当に前記の IDコードもしくはパスワードを知得すれば任意の端末デバイスから容易に当該機密情報にアクセスし、これを詐取することは必ずしも不可能ではなく、實際上、当該機密情報にアクセスして来た端末デバイス自体の正当性を確認することは、別途電話通信による逆探知手法によるとしても、相当の所要時間を費やすこととなり、この端末デバイスそのものの正当性を確認することは殆ど不可能であるため、機密情報の伝送処理には、不安がつきまうものであった。

【0004】 このような不安を解消するための具体的な改善例としては、例えば、特開昭 63-155930 号公報（公知例）の発明が知られている。

【0005】 この公知例のデータ暗号化通信方式は、公衆データ網を利用して、プロトコル変換手段により変換されたデータを、暗号化キーを付加情報としたパケットとして伝送し、保有する復号化手段の特定キーに基づいてデータの復号化を図るようになしたものである。

【0006】

【発明が解決しようとする課題】 前記の公知例のものにあっては情報も暗号化して、これを伝送するものであるが、その目的とするところは、暗号化手段を保有しないデバイス間で公衆データ網を利用して暗号化データを伝送するものであるから、不特定の第三者によるデータ通信デバイスを用いた暗号化情報へのアクセスはフリーとなり、重要な情報の漏洩を完全に未然防止する点での不安が残るものであり、機密情報の伝送に携わるユーザ側からは、暗号化情報が特定の正当な端末デバイス間においてのみ授受されることが保障されるように、その

保有する端末デバイスの登録、確認を図って常時安心して機密情報の保管・伝送が可能な情報伝送手法の提供が切望されており、この発明の目的とするところは、かかるユーザニーズに応えうる、以下の如き優れたシステムを提供することである。

【0007】(1) 機密情報を暗号化処理して安全に伝送可能である。

【0008】(2) 情報伝送に関与できる端末デバイスを予め登録し、利用される端末デバイスの正当性を確認した後に機密情報を伝送させるため、IDコードやパスワードなどを知得しただけでは機密情報にアクセスすることは出来ない。

【0009】(3) 端末デバイスの登録・確認に際して、活用される暗号化端末識別キーを創成する端末識別キーを乱数キーによって復号化し、さらに認証キーによってこれを暗号化処理したものであるため、機密情報の発信側と受信側の双方において、前記暗号化端末識別キーの守秘性が確保され、機密情報の漏洩を未然防止しうるものである。

【0010】

【課題を解決するための手段】前記の目的を達成するための、この発明の構成について見れば、次の通りである。

【0011】(1) 予め登録された正当な端末デバイス間で情報を伝送しうる情報伝送システムであって、前記の端末デバイスには、暗号デバイスを接続しており、個々のユーザ暗証を暗号アルゴリズムにより暗号化処理して前記の端末デバイスを特定しうる端末識別キーを創成し、当該端末識別キーにより端末デバイスの正当性を確認した後、情報を伝送するように構成した情報伝送システム。

【0012】(2) 端末デバイスを備えたファイルサーバ手段と、ファイルレシーバ手段との間に同様の端末デバイスを備えたセキュリティサーバ手段を介在させて、情報を授受しうるようにした前記(1)記載の情報伝送システム。

【0013】(3) 前記セキュリティサーバ手段においては、前記ファイルサーバ手段と、ファイルレシーバ手段とに乱数キーを送信しうる手段と、前記ファイルサーバ手段とファイルレシーバ手段とから返信された端末識別暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより前記ファイルサーバ手段と、ファイルレシーバ手段の暗号化端末識別キーを登録しうる手段を備えており、前記ファイルサーバ手段と、ファイルレシーバ手段においては、各端末識別キーの創成と、各端末識別キーを前記乱数キーによって暗号化して端末識別暗号キーを創成して、これを前記セキュリティサーバ手段に返信しうる手段とを備えた前記(1)又は(2)記載の情報伝送システム。

【0014】(4) 前記セキュリティサーバ手段にあって

は、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して照合キーを生成すると共に、前記ファイルサーバ手段から返信された端末識別キーによって乱数キーを暗号化した確認キーと、当該照合キーとを照合させて、前記ファイルサーバ手段の端末デバイスの正当性を認証しうる手段を具備してなる前記(1)乃至(3)記載の情報伝送システム。

【0015】(5) 前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して暗号処理キーを求めると共に、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して復号化処理キーを生成する手段を備えており、当該暗号化処理キーをファイルサーバ手段に送信し、ファイルサーバ手段においては、その端末識別キーにより前記暗号化処理キーを復号化して暗号化実行キーを生成し、当該暗号化実行キーにより機密ファイルを暗号化して、前記セキュリティサーバ手段に返信しうる手段を含んでいる前記(1)乃至(4)記載の情報伝送システム。

【0016】(6) 前記セキュリティサーバ手段にあっては、前記暗号化ファイルと共に、前記復号化処理キーをファイルレシーバ手段に送信する手段を含んでおり、ファイルレシーバ手段にあっては、その端末識別キーにより復号化処理キーを復号化して復号化実行キーを求め、当該復号化実行キーにより、暗号化ファイルを復号化処理して平文情報を受領しうる手段を備えている前記(1)乃至(5)記載の情報伝送システム。

【0017】

【作 用】この発明の構成は以上の通りであって、予め暗号化処理して創成された端末識別キーを利用して暗号化端末識別キーを登録し、情報伝送の際には、利用端末デバイスの正当性を確認した後、暗号化された情報を発信させ、当該情報を受信する側に対しても、正当な登録済みの端末デバイスのみが解読しうる復号化処理キーと共に暗号化情報を提供し、受信する側の正当な端末デバイスにおいて平文情報化するものである。

【0018】

【実施例】次に、この発明の実施例を図面に基づいて説明する。図1には、この実施例の情報伝送システム(1)に関する機能ブロック図が示されており、当該システム(1)を構成するセキュリティサーバ手段(10)は、公衆電話回線、LANあるいはISDN回線などの公衆通信網(N)を利用して、多数のファイルサーバ手段(100)ならびにファイルレシーバ手段(200)に接続されたものである。

【0019】前記セキュリティサーバ手段(10)の構成は、中央デバイス(11)と当該中央デバイス(11)に暗号デバイス(12)を結線したものであって、

その機能としては、ファイルサーバ手段(100)およびファイルレシーバ手段(200)における各端末デバイス(101)、(201)間の暗号情報の授受を可能とするものであるが、その詳細は後述する。

【0020】更に、前記ファイルサーバ手段(100)側においては、端末デバイス(101)…と、当該端末デバイス(101)…に個別に接続された暗号デバイス(102)を含んだ構成とされており、その機能としては、各端末デバイス(101)の登録ならびに暗号情報の授受を可能としたものであるが、その詳細についても後述する。

【0021】又、前記ファイルレシーバ手段(200)についても、本質的に前記ファイルサーバ手段(100)の場合と同様に端末デバイス(201)…および暗号デバイス(202)を含んだ構成とされているものである。

【0022】従って、必要に応じては、前記ファイルサーバ手段(100)とファイルレシーバ手段(200)とが立場を換えて、前記ファイルレシーバ手段(200)

$$KO = D_z \{ E_y (X) \} \dots \dots \dots \text{式1}$$

【0027】即ち、この式1の内容は、情報(X)を暗号キー(Y)により暗号化(エンサイファー)し、更に、暗号キー(Z)により復号化(デサイファー)した結果は、函数出力(KO)としてとらえることを意味するものである。

【0028】① 端末デバイスの登録

先ず、情報の伝送に先立って、前記の端末デバイス(101)(201)の登録を実施しなければならない。

【0029】その理由は、貴重な機密情報をハンドリングするオペレータについては、パスワードもしくはIDコードなどによって確認されるとしても、当該オペレータにより特定の端末デバイスが正当に操作されていることが確認された場合に限りて端末デバイスが機能し、情報伝送が可能となるようにすることが情報の漏洩防止のために重要であるが故である。

【0030】即ち、この点を換言すれば、予め情報伝送処理に関与することが許諾された登録済みの正当な端末デバイス間のみで情報伝送が可能であるから、前記パスワードやIDコードなどによるオペレータの確認と併用することにより、情報の機密保持が一層確実に保障されることとなるものである。

【0031】そこで、以下にこの登録の手順を図2および図3に示すフローチャートをも参照して説明する。

【0032】(1) 端末識別キー(ESK)(ERK)の創成

端末識別キー(ESK)(ERK)とは、前記第1の企業と第2の企業が保持する秘密の独自の「キー」であって、以下に述べるような手順で創成し、これを秘密の状態で作成するものである。

0)から前記ファイルサーバ手段(100)に対して暗号情報を提供することが可能であることは容易に理解されるところである。

【0023】尚、図1において、(13)はメモリ手段であって、セキュリティ管理表(14)を含むものである。

【0024】次に、この実施例のシステム(1)におけるファイルサーバ手段(100)とファイルレシーバ手段(200)の端末デバイス(101)(201)の登録・認証ならびに暗号情報の伝送について、第1の企業をファイルサーバ、又第2の企業をファイルレシーバと仮定し、各々の端末デバイス(101)と(201)との間の伝送処理のケースを例に挙げて説明すると次の通りである。

【0025】なお、この出願明細書における情報の暗号化ならびに復号化に関する数式は、式1によるものと定義する。

【0026】

【数1】

式1

【0033】まず、各端末デバイス(101)(201)において、0~9の9個の数字と、A~Fの6個のアルファベットの合計16桁の記号群の16乗(16¹⁶)の乱数から任意の記号群を選定してユーザ固有のユーザ暗証(SK)(RK)を決定し、当該端末デバイス(101)(201)に接続された暗号デバイス(102)(202)により前記ユーザ暗証(SK)(RK)を暗号アルゴリズム(AL)によって、端末識別キー(ESK)(ERK)を創設する(SP1)、(SP2)。

【0034】尚、前記の暗号アルゴリズムについては、例えば、1977年以来、開示済みの米国標準「DES(DATA ENCRYPTION STANDARD)」あるいは、NTT社による「FEAL8システム」の如き8バイトを単一のブロックとするブロック暗号化方式のものを利用することが便利であり、これらの暗号アルゴリズム(AL)については公開されているが、当該アルゴリズムに使用する「キー」であるユーザ暗証(SK)(RK)を秘密に保持することにより、当該「キー」を知る者以外の者には解読できない仕組みとなっているため、その守秘性は安全に保障されうるものである。

【0035】前記の如く、後述の情報伝送に際しての、各端末デバイス(101)(201)の認証のために重大な判定要素となる端末識別キー(ESK)(ERK)は、暗号化アルゴリズムによって暗号化処理されているため、第三者によって視認され、もしくは解読されるおそれは皆無であって、秘密保持の安全性は極めて高いものであると言える。

【0036】(2) 端末デバイス(101)(201)の登録

次に、図3に示すフローチャートに基づいて、端末デバイス(101)(201)をセキュリティサーバ手段(10)に登録する手順について述べると次の通りである。

【0037】まず、端末デバイス(101)(201)を操作して中央デバイス(11)に対して、端末登録の請求を行なう(SP5)。

【0038】この登録請求を受理したセキュリティサーバ手段(10)においては暗号デバイス(12)から提供された格別の意味を持たない乱数キー(RR)を、

$$SS = E_{RR}(ESK)$$

【0041】

$$RS = E_{RR}(ERK)$$

【0042】次に、セキュリティサーバ手段(10)においては、各端末デバイス(101)(201)の暗号化端末識別キー(SZ)(RZ)の登録を行なうこととなるが、その内容は、暗号デバイス(12)において端末識別暗号キー(SS)(RS)を乱数キー(RR)によって復号化し、更にこれを認証キー(CK)により暗

$$SZ = E_{CK}[D_{RR}(SS)]$$

【0044】

$$RZ = E_{CK}[D_{RR}(RS)]$$

【0045】となり、これを、中央デバイス(11)に登録し、メモリ手段(13)にあるセキュリティ管理表(14)に格納・保管することにより、端末デバイス(101)(201)の登録が完了する(SP8)。

【0046】② 暗号情報の授受

次に、端末デバイス(101)から平文情報の機密ファイル(FL)を端末デバイス(201)へ伝送する場合について見れば、図4に示す通りである。

【0047】(1) 端末デバイス(101)の確認

【0048】まず、端末デバイス(101)から中央デバイス(11)に対して機密ファイル(FL)の伝送請求がなされる(SP9)。

【0049】セキュリティサーバ手段(10)において

$$ESK = D_{CK}(SZ) \quad \dots \dots \dots \text{式6}$$

【0052】

$$MK = E_{ESK}(RR) \quad \dots \dots \dots \text{式7}$$

【0053】一方、前記の乱数キー(RR)を受信した端末デバイス(101)においては、暗号デバイス(102)によって当該乱数キー(RR)を端末識別キー

それぞれ前記端末デバイス(101)(201)に送信する(SP6)。

【0039】前記の乱数キー(RR)を受信した前記端末デバイス(101)(201)においては、それぞれの暗号デバイス(102)(202)において、端末識別キー(ESK)(ERK)を、乱数キー(RR)によって暗号化して端末識別暗号キー(SS)(RS)作成し、これを中央デバイス(11)へ返信する(SP7)。この点は、次の式に示す通りである。

【0040】

【数2】

$$\dots \dots \dots \text{式2}$$

【数3】

$$\dots \dots \dots \text{式3}$$

号化して各端末デバイス(101)(201)の暗号化端末識別キー(SZ)(RZ)を生成するものであって、その式は次の通り、

【0043】

【数4】

$$\dots \dots \dots \text{式4}$$

【数5】

$$\dots \dots \dots \text{式5}$$

は、この請求が真正な端末デバイス(101)からなされたものであることを確認するために、乱数キー(RR)を端末デバイス(101)へ送信すると共に、照合キー(MK)を内製する(SP10)。

【0050】この照合キー(MK)の内製の手順については、端末デバイス(101)の暗号化端末識別キー(SZ)を認証キー(CK)によって復号化し、求められた端末識別キー(ESK)によって乱数キー(RR)を暗号化して生成するものであって、その式は次の通りとなる。

【0051】

【数6】

$$\dots \dots \dots \text{式6}$$

【数7】

$$\dots \dots \dots \text{式7}$$

(ESK)で暗号化処理して確認キー(SA)を作成し、セキュリティサーバ手段(10)へ返信する(SP11)のものであり、その式は次の通りである。

【0054】

$$SA = E_{ESK} (RR) \dots \dots \dots \text{式8}$$

【0055】その後、この確認キー (SA) を前記照合キー (MK) と照合し (SP12)、その結果が一致すれば、ファイル伝送請求が第1の企業の端末デバイス (101) からなされたものであることが確認され、ファイル伝送が許可されることとなるが (SP13)、この照合の結果が不一致であれば、例えば、図示しない表示、警報手段などにより報知せしめるものである (SP14)。

【0056】なお、この照合作業に併せて、第1の企業の端末デバイス (101) のオペレータに関して、例えば、IDコードやパスワードなどを照合させ、その合致を確認することにより、尚一層の情報の漏洩防止に寄与

$$ESK = D_{CK} (SZ) \dots \dots \dots \text{式9}$$

【0059】次で、この端末識別キー (ESK) により乱数キー (RR) を暗号化して、暗号化処理キー (AAK) を得るものであるが、この式は次の通りである。

$$AAK = E_{ESK} (RR) \dots \dots \dots \text{式10}$$

【0061】又、更に、中央デバイス (11) においては、機密ファイル (FL) の伝送先である端末デバイス (201) における暗号デバイス (202) の復号化処理キー (BBK) をも作成するが、その操作は、その暗号化端末識別キー (RZ) を認証キー (CK) で復号化

$$ERK = D_{CK} (RZ) \dots \dots \dots \text{式11}$$

【0063】

$$BBK = E_{ERK} (RR) \dots \dots \dots \text{式12}$$

【0064】この復号化処理キー (BBK) はメモリ手段 (13) に保存するとともに、前記の暗号化処理キー (AAK) のみを端末デバイス (101) へ送信する (SP15)。

【0065】この暗号化処理キー (AAK) を受理した端末デバイス (101) においては、暗号デバイス (102) において、

$$AAZ = D_{ESK} (AAK) \dots \dots \dots \text{式13}$$

【0067】又、この暗号化実行キー (AAZ) により機密ファイル (FL) を暗号化して、暗号化ファイル (AFL) を作成する (SP16) ものであり、次式の

$$AFL = E_{AAZ} (FL) \dots \dots \dots \text{式14}$$

【0069】次に、端末デバイス (101) により、この暗号化ファイル (AFL) をセキュリティサーバ手段 (10) に送信する。

【0070】この暗号化ファイル (AFL) を受信したセキュリティサーバ手段 (10) においては、当該暗号化ファイル (AFL) と共に前記の復号化処理キー (BBK) についても端末デバイス (201) へ送信する (SP17)。

$$BB = D_{ERK} (BBK) \dots \dots \dots \text{式15}$$

【0074】次で、この復号化実行キー (BBZ) により暗号化ファイル (AFL) を復号化して、機密ファイ

ル (FL) を平文情報に復帰させて受領しうるものである。次で、この復号化実行キー (BBZ) により暗号化ファイル (AFL) を復号化して、機密ファイ

【0057】(2) 機密ファイルの伝送

次に、機密ファイル (FL) の伝送請求を受理したセキュリティサーバ手段 (10) においては、端末デバイス (101) 特有の暗号化処理キー (AAK) を生成し、これを端末デバイス (101) へ送信することとなるが、その操作は、暗号化端末識別キー (SZ) を認証キー (CK) で復号化して端末識別キー (ESK) を生成することとなるが、その式は次の通りとなる。

【0058】

$$\dots \dots \dots \text{式9}$$

【0060】

【数10】

して得られた端末識別キー (ERK) によって、乱数キー (RR) を暗号化して復号化処理キー (BBK) を生成するものであって、次の式に示す通りである。

【0062】

【数11】

$$\dots \dots \dots \text{式11}$$

【数12】

03) により暗号化処理キー (AAK) を端末識別キー (ESK) により復号化することにより暗号化実行キー (AAZ) を生成する (SP16) ものであり、次式の通りである。

【0066】

【数13】

$$\dots \dots \dots \text{式13}$$

通りである。

【0068】

【数14】

$$\dots \dots \dots \text{式14}$$

【0071】(3) ファイルの受信と復号化

【0072】次に、これらの送信を受けた端末デバイス (201) 側の暗号デバイス (202) においては、復号化処理キー (BBK) を、端末識別キー (ERK) によって復号化して、復号化実行キー (BBZ) を得るが、これは次式の通りである (SP18)。

【0073】

【数15】

$$\dots \dots \dots \text{式15}$$

ル (FL) を平文情報に復帰させて受領しうるものである。次で、この復号化実行キー (BBZ) により暗号化ファイル (AFL) を復号化して、機密ファイ

【0075】

$$FL = D_{BBZ} (AFL) \dots \dots \dots \text{式16}$$

【0076】なお、この実施例においては、第1の企業と第2の企業に設置された特定の端末デバイス間における情報の伝送処理について記述したが、これ以外に、例えば、本社と支社、あるいはホームバンキングの如く金融機関と端末手段を設置した一般家庭の間においても、同様に機密情報の授受をなしうるものであることは言うまでもないことである。

【0077】又、前記の実施例においては、その技術内容の理解を助成するためにファイルサーバ手段(100)と、ファイルレシーバ手段(200)とを単一対状に図示して説明したが、ファイルサーバ手段(100)とファイルレシーバ手段(200)とは、適宜複数個併設し、それらの間で情報の授受をなしうるよう構成しうことは詳しく説明するまでもなく当然のことであり、ファイルサーバ手段(100)のみならず、ファイルレシーバ手段(200)のいずれにも、暗号デバイス(102)(202)が接続されているから、機密情報をセキュリティサーバ手段(10)を仲介することなく、ファイルサーバ手段(100)からファイルレシーバ手段(200)へ直接に機密情報を伝送するように操作することも可能なことであることは、重ねて説明するまでもないことである。

【0078】

【発明の効果】以上の通り、この発明によれば、平文情報を暗号化処理して機密の状態与安全に伝送されるばかりでなく、情報の授受に関係する端末デバイスが予め登録された端末識別キーを具備していることを認証することによって、正当な端末デバイスであることが確認された後に、暗号化された情報の発信を実行するものであり、加えて、情報を受信する側の端末デバイスについても、同様に正当な登録を受けた端末デバイスに限って情報を受領し、その解読のための復号化処理キーの提供をうけて、当該暗号化情報を平文情報に解読できるものであり、完璧に機密状態で情報の授受が可能である。

【0079】又、暗号化端末識別キーを創成する端末識

【数16】

別キーがユーザ暗証と暗号アルゴリズムによって創成するものであるから、端末識別キーの秘密保存が安全に保障されて機密情報の漏洩の防止を一層確実にさせうるものである。

【図面の簡単な説明】

【図1】この発明の実施例を示す機能ブロック図。

【図2】図1における端末識別キー創成のフローチャート。

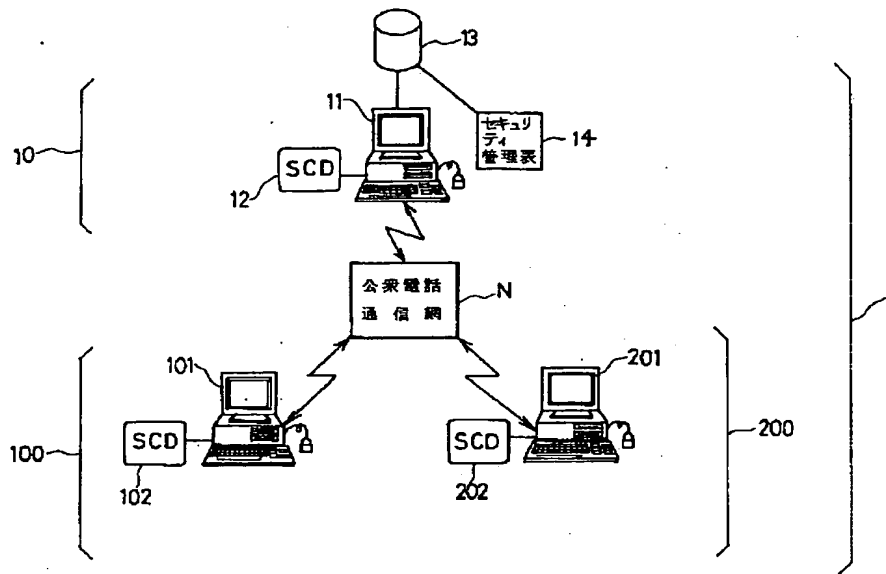
【図3】図1における端末登録のフローチャート。

【図4】図1における情報伝送のフローチャート。

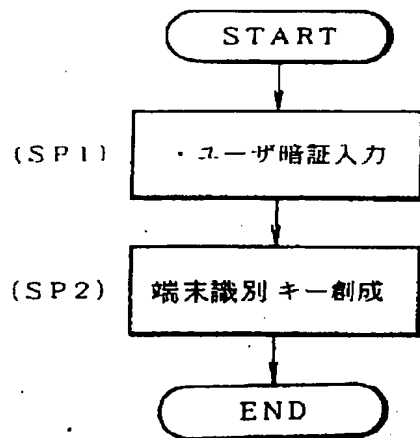
【符号の説明】

1	情報伝送システム
10	セキュリティサーバ手段
11	中央デバイス
101, 201	端末デバイス
12, 102, 202	暗号デバイス
13	メモリ手段
100	ファイルサーバ手段
200	ファイルレシーバ手段
AL	暗号アルゴリズム
SK, RK	ユーザ暗証
SZ, RZ	暗号化端末識別キー
SS, RS	端末識別暗号キー
ESK, ERK	端末識別キー
SA, RA	確認キー
RR	乱数キー
FL	機密ファイル
AFL	暗号化ファイル
MK	照合キー
CK	認証キー
AAK	暗号化処理キー
AAZ	暗号化実行キー
BBK	復号化処理キー
BBZ	復号化実行キー

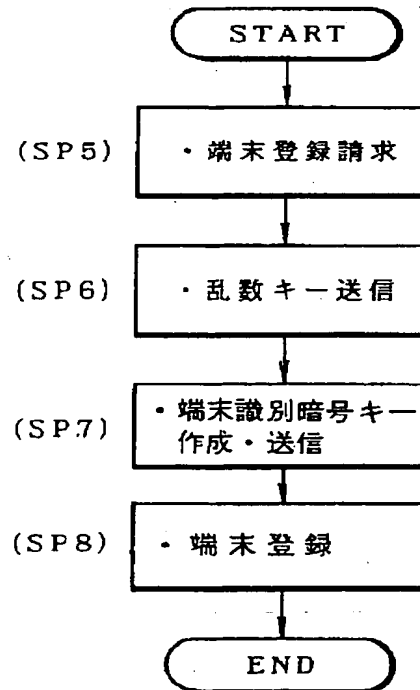
【図 1】



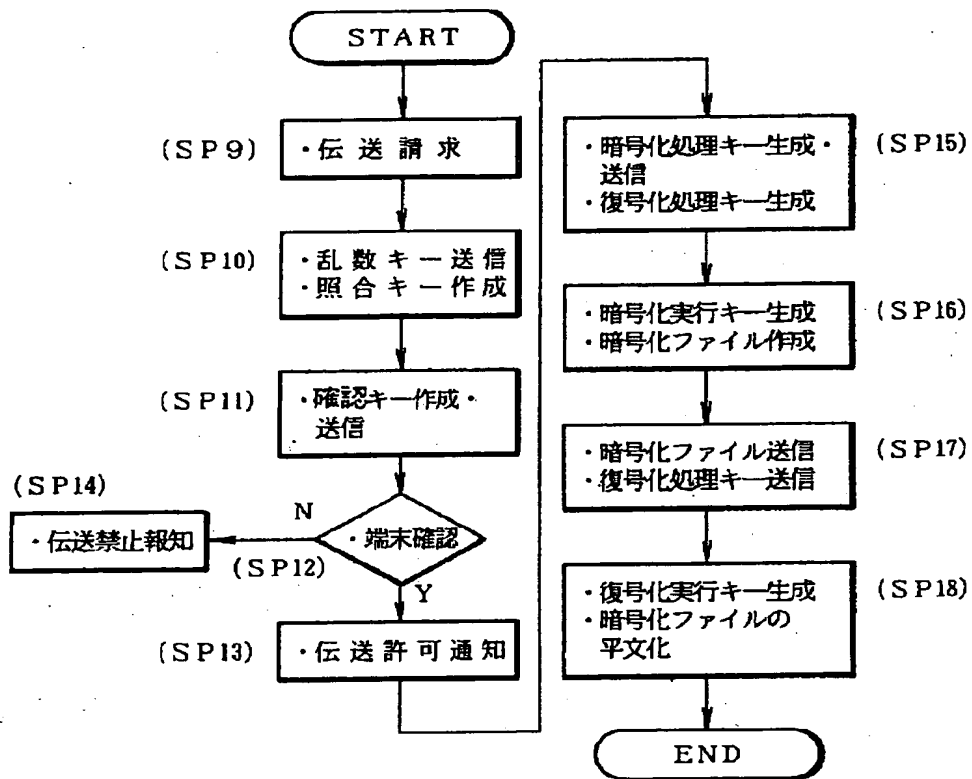
【図 2】



【図 3】



【図 4】



フロントページの続き

(51) Int. Cl. 6

H 0 4 L 9/10

9/12

9/14

識別記号

庁内整理番号

F I

技術表示箇所

BEST AVAILABLE COPY